European Journal of Risk Regulation (2023), 1–21
doi:10.1017/err.2023.58

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach

Sébastien Fassiaux

Universitat Pompeu Fabra, Barcelona, Spain
Email: sebastien.fassiaux@upf.edu

Abstract

Personal autonomy is at the core of liberal societies, and its preservation has been a focus of European Union (EU) consumer and data protection law. Professionals increasingly use artificial intelligence in consumer markets to shape user preferences and influence their behaviours. This paper focuses on the long-term impact of artificial intelligence on consumer autonomy by studying three specific commercial practices: (1) dark patterns in user interfaces; (2) behavioural advertising; and (3) personalisation through recommender systems. It explores whether and to what extent EU regulation addresses the risks to consumer autonomy of using artificial intelligence in markets in the long term. It finds that new EU regulation does bring novelties to protect consumer autonomy in this context but fails to sufficiently consider the long-term consequences of autonomy capture by professionals. Finally, the paper makes several proposals to integrate the long-term risks affecting consumer autonomy in EU consumer and data protection regulation. It does so through an interdisciplinary approach, drawing from legal research and findings in the study of long-term thinking, philosophy and ethics and computer science.

Keywords: Artificial intelligence; autonomy; consumers; long-term thinking

I. Introduction

The short-term thinking driving policymaking and business decisions contributes to the major crises that our societies are currently facing. A growing body of academic literature addresses the need for long-term thinking in various policy areas,[1] including the risks that artificial intelligence (AI) poses to society.[2] AI researchers sometimes disagree on the time frame to assess this technology: to focus on either its present or future risks and impacts. However, Baum suggests realigning the debate around an "intellectualist" faction – developing AI and assessing its risks for the sake of intellectual interest – and a

[1] C Winter et al, *Legal Priorities Research: A Research Agenda*, Legal Priorities Project, January 2021, <https://www.legalpriorities.org/research_agenda.pdf> (last accessed 4 January 2023).

[2] ibid, 35–55 and the literature cited. See also C Prunkl and J Whittlestone, "Beyond Near- and Long-Term: Towards a Clearer Account of Research Priorities in AI Ethics and Society" (2020) *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* <https://doi.org/10.1145/3375627.3375803> 138–43; L Bjørlo, Ø Moen and M Pasquine, "The Role of Consumer Autonomy in Developing Sustainable AI: A Conceptual Framework" (2021) 13(4) Sustainability 2332.

"societalist" faction – studying the societal impacts in both the near and long term.[3] Here, the focus is to assess the near- and long-term risks associated with using AI in consumer markets, in line with the latter approach. As developed below, various time scales are thus relevant when analysing these risks: some risks can materialise soon (eg risks for today's children), while others can take decades or generations to emerge (eg risks for cultural transmission). Uncertainty in the face of rapid technological development is also relevant to this discussion. Ultimately, this exercise also relates to the sustainability of AI; that is, "the extent to which AI technology is developed in a direction that meets the needs for the present without compromising the ability of the future generations to meet their own needs".[4]

AI is intrinsically linked to future thinking, as the technology learns from past and present data to predict future outcomes. Deep learning, an AI technique based on artificial neural networks, allows AI systems to learn autonomously from a given dataset. Firms use AI to predict consumer preferences and behaviours and influence transactional decision-making in consumer markets. To some extent, traditional marketing (ie before the uptake of digital technologies and big data) had the same objectives. However, the unprecedented ability of AI technologies to predict consumer preferences and influence transactions and the scale at which firms have been using AI for marketing purposes warrant specific research and assessment of the current legal and regulatory landscape in this field.[5]

Indeed, in some instances, new AI-enabled commercial practices unjustifiably affect consumer autonomy, here understood as their ability to make decisions without undue commercial influence. The focus here is on three undue commercial practices: (1) the use of so-called "dark patterns" – or manipulative design – in user interfaces; (2) abuses in behavioural advertising; and (3) the lack of control over personalised services through recommender systems. Reflecting on the risks and impacts of AI on consumer autonomy in the near and long term is of paramount importance in liberal democracies[6] because its preservation is one of European Union (EU) consumer and data protection law's foundations.[7]

Therefore, this article first briefly conceptualises consumer autonomy (Section II). Second, it evaluates near- and long-term risks of AI-driven influences on consumers' autonomy (Section III). Third, it maps and assesses the EU regulatory instruments addressing these risks to consumer autonomy (Section IV). Fourth, it concludes with a set of proposals for integrating these concerns into EU regulations (Section V). The article takes an interdisciplinary approach, drawing from legal and regulatory considerations and findings in the study of behavioural economics, philosophy and ethics and computer science.

II. Conceptualising consumer autonomy

The concept of autonomy is central to the EU's consumer and data protection law framework, but it appears to lack a proper definition, which makes it difficult to

[3] SD Baum, "Reconciliation between factions focused on near-term and long-term artificial intelligence" (2018) 33 AI & Society 565.

[4] Bjørlo et al, supra, note 2, 7. The authors apply this definition to the future of consumer autonomy and decision-making.

[5] On this point, see E Mik, "The Erosion of Autonomy in Online Consumer Transactions" (2016) 8(1) Law, Innovation and Technology 22–24.

[6] Zuboff claims that individuals have a "right to the future tense": the right to decide for their own future, without undue commercial influence and privacy intrusions, which is at the core of the idea of free will (S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London, Profile Books 2019) pp 328–47). See also J Raz, *The Morality of Freedom* (Oxford, Oxford University Press 1986) pp 400–29; B Roessler, *Autonomy: An Essay on the Life Well Lived* (Cambridge, Polity 2021) p 62.

[7] HW Micklitz, "The General Clause on Unfair Practices" in G Howells, HW Micklitz and T Wilhelmsson (eds), *European Fair Trading Law: The Unfair Commercial Practices Directive* (Abingdon, Routledge 2006) p 104.

understand.[8] In turn, a lack of a proper conceptualisation of consumer autonomy entails a systemic difficulty for policymakers to properly calibrate regulation to the realities generated by new technologies. This regulatory struggle is especially true in the AI context, which is characterised by the rapid evolution of technologies, new challenges for individual consumers and risks for society at large. As the following sections develop, these collective risks – resulting from the spillover from individual infringements into societal issues – inter alia consist in the increased economic power in the hands of a few concentrated businesses, threats to democracy and alterations to the formation of human personality. This collective dimension should properly be considered in conceptualising consumer autonomy in the AI context.

Despite its legal connotations, better understanding the concept of autonomy requires "a reference point outside the legal system",[9] mainly because of its meaning in private law – usually referring to the freedom of contract – which is too narrow. It is thus appropriate to better conceptualise autonomy from an interdisciplinary viewpoint, as follows, with relevant references to the marketing, ethics and sustainability literature, moving from a general context to a more specific AI one. A more original conceptualisation applied to AI marketing is offered hereafter.

Classically, autonomy refers to the ability to govern oneself, free from external control or manipulation – thus implying independence.[10] The marketing literature is particularly relevant to conceptualising autonomy applied to consumers. As in EU law, autonomy also appears to lack proper conceptualisation in marketing ethics.[11] A literature review of this field reveals that authors define autonomy as involving control, will and desire, choice and self-reflection.[12] More importantly, consumer autonomy is the ethical precondition that legitimates marketing as a social system in capitalistic societies.[13] Building on existing research in marketing theory, Anker distinguishes between internal and external conditions for consumer autonomy and suggests that consumers are more likely to be autonomous when they have access to relevant information and can critically reflect on it based on their values and goals.[14] At the same time, it is well established that consumer autonomy is affected by cognitive limitations[15] and social contexts.[16] In consumer law, these limitations have challenged the regulatory focus on information requirements partly based on the belief that consumers are perfectly rational agents who do read the fine print.[17]

Looking at autonomy from an ethical perspective helps further flesh out the concept. Sax et al have laid down three requirements for consumer autonomy in a digital context: (1) *independence* – being in control of one's life by acting based on one's own "values,

[8] A Jabłonowska, M Kuziemski, AM Nowak et al, "Consumer Law and Artificial Intelligence: Challenges to the EU Consumer Law and Policy Stemming from the Business' Use of Artificial Intelligence, Final Report of the ARTSY Project", *EUI Working Papers LAW 2018/11*, 12; T Anker, "Autonomy as License to Operate: Establishing the Internal and External Conditions of Informed Choice in Marketing" (2020) 20(4) Marketing Theory 528.

[9] Micklitz, supra, note 7; M Sax, N Helberger and N Bol, "Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices" (2018) 41 Journal of Consumer Policy 103; Jabłonowska et al, supra, note 8, 14.

[10] See J Christman, *Autonomy in Moral and Political Philosophy* (The Stanford Encyclopedia of Philosophy, 2020), EN Zalta (ed.) <https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/> (last accessed 8 May 2023). See also Raz, supra, note 6; Roessler, supra, note 6.

[11] MR Hyman, A Kostyk and D Trafimow, "True Consumer Autonomy: A Formalization and Implications" (2023) 183 Journal of Business Ethics 841.

[12] ibid.

[13] Anker, supra, note 8.

[14] ibid.

[15] A Alemanno and AL Sibony (eds), *Nudge and the Law: A European Perspective* (Oxford, Hart Publishing 2015).

[16] See Roessler, supra, note 6, 154–76.

[17] Y Bakos, F Marotta-Wurgler and DR Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts" (2014) 43(1) Journal of Legal Studies 1.

desires and goals"; (2) *authenticity* – truly identifying with one's own values, desires and goals, free from manipulation; and (3) *options* – allowing for effectively acting based on one's own values, desires and goals, which would otherwise remain useless.[18] This definition aligns with the marketing literature review mentioned above: in order for consumer transactions to reflect their wills and desires, they first need to have sufficient options and true choices. The importance of choices brought by competition is an aspect of consumer autonomy that is sometimes overlooked.

Moreover, consumer autonomy has been defined by scholars when studying the sustainability of AI systems, which is relevant when considering the long-term impacts of AI technologies on consumers. Bjørlo et al argue that consumer autonomy in this context requires: (1) *transparency* – consumers must understand how AI systems make decisions and what information they are using; (2) *complementarity* – consumers should be able to use AI systems actively to augment their autonomy, not only as passive receivers of recommendations, for instance; and (3) *privacy regulation* – to ensure that firms do not exploit personal data to feed their AI systems.[19] The authors again point to the collective dimension of autonomy preservation through privacy, the individual protection of which has positive spillover effects on society at large.[20] In an AI context, the issue of privacy is unavoidable, as AI systems affecting consumer autonomy rely on the large-scale collection and processing of personal data. The definition also offers a more specific focus on interactions between consumers and AI systems, which is relevant in this context because, by definition, AI systems do operate with varying degrees of autonomy themselves.

Building on these preliminary definitions of consumer autonomy, one can propose a more comprehensive conception that also takes long-term risks into account. The idea behind this concept is that if consumer autonomy is the ethical precondition legitimising marketing as a social system in capitalistic societies, then AI marketing must respect consumer autonomy to remain legitimate. The conception proposed here relies on four requirements for preserving consumer autonomy in the context of AI marketing: (1) choice; (2) privacy; (3) independence; and (4) reciprocity (see Figure 1). Without ordering them hierarchically – no requirement is more important than the other – each subsequent requirement is the precondition for the next. In that sense, this framework allows us to put these requirements in relation: some harms to consumer autonomy require remedies that pertain to other requirements upstream.

First, the requirement of *choice* implies both structural and granular elements. Structurally, choice implies the need for sufficient competition. Otherwise, limited options can structurally thwart autonomous action. Lack of competition is already a challenge today: powerful actors dominate many AI-intensive consumer markets, and national and EU competition enforcement has been taking place in many of them, including search engines, targeted advertising and app stores. More competition in consumer markets using AI would allow more choices for consumers. In a data-intensive context, more competition can be fostered through the right to data portability, for instance. At a more granular level, choice implies true options for consumers when transacting and defining the limits of that transaction without professionals manipulating these options. In turn, both structurally and granularly, privacy could become more of a differentiating factor between competitors. In the long term, more competition and privacy-friendly consumer choices would encourage more trustworthy innovation.

Second, *privacy* has become increasingly relevant with the development of information technologies and even more so in the AI context. In many markets lacking effective competition, consumers have fewer options and are often attracted to platforms whose

[18] Sax et al, supra, note 9.

[19] Bjørlo et al, supra, note 2.

[20] C Véliz, *Privacy is Power* (London, Bantam Press 2020) pp 75–82.

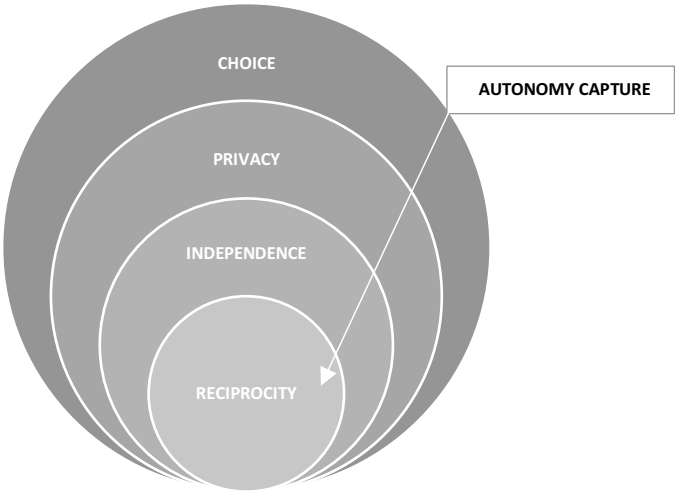

Figure 1. Capture of the four requirements for consumer autonomy.

business models mainly rely on the extensive collection and processing of personal data – including for behavioural advertising – against free services. Hence the need to analyse the impacts of AI on consumer autonomy by considering both consumer and data protection laws. This reality has two consequences in terms of autonomy. On the one hand, the large scale of individual privacy violations has significant consequences for society. For instance, misusing large amounts of personal data has enabled interferences in the democratic political process. The spillover from individual data protection infringements into societal issues, again, refers to a more collective dimension of consumer autonomy. On the other hand, respect for consumer privacy is a precondition to their independence in market transactions, free from manipulation.

Third, *independence* can be seen as a shield of consumer autonomy. Having more control over their personal data, consumers can better preserve their preferences and desires when consuming content, thus preserving their authenticity and avoiding manipulation. More control implies, for instance, more transparency from AI marketing actors, protection against exposure to biased content, access to the parameters of algorithmic decision-making in an intelligible way and clear labels and information requirements. To preserve effective consumer autonomy, more transparency should be coupled with the ability to withdraw from targeting or personalised services. With the long term in mind, preserving consumer independence implies clear rules and prohibitions around the use of generative AI in marketing. In turn, consumer independence is a prerequisite for more reciprocity between contracting parties when AI systems are involved.

Finally, *reciprocity* can be seen as the sword of consumer autonomy. More independence upstream means a greater ability for consumers to play on a more level playing field with professionals using AI marketing downstream. More reciprocity implies the possibility for consumers who do choose targeting and personalisation to engage in a more complementary – and active – way with AI services (eg with the possibility of controlling specific parameters of the advertisements shown to consumers, the recommendations they receive or the chatbots they interact with). Giving consumers more control over the adequacy of the AI-recommended content would indeed be autonomy-enhancing.

Analysing consumer autonomy through this four-layer prism also allows us to study the dynamic at play. The argument here is that the current situation in consumer markets allows "autonomy capture" by professionals using AI systems at the expense of consumers.

This autonomy capture first occurs at a more structural level of market competition and individual choices about transactions. Then, it progressively affects the subsequent requirements of privacy and independence to reach the reciprocity in the relationship between individual consumers and businesses. In this setting, each requirement is a prerequisite for the next because they form a progression that safeguards and enables consumer autonomy. Choice establishes the foundation for autonomy, privacy ensures the protection of personal information and independence and independence empowers consumers to engage reciprocally with AI systems. Together, these requirements create a framework that allows consumers to exercise autonomy in their interactions with AI marketing. The understanding of the dynamic of autonomy capture at play helps us analyse the applicable regulatory framework and find new remedies against AI-generated harms to consumer autonomy. The following analysis is conducted against the conceptualisation of consumer autonomy proposed here.

III. Long-term risks to consumer autonomy posed by artificial intelligence

Undoubtedly, consumers can benefit from AI systems and personalisation, as it allows them to make sense of the vast amounts of information and content available. Therefore, AI systems can improve consumer autonomy by making more relevant information available, allowing more efficient and accessible decision-making based on more personalised options. If these systems were transparent, complementary and allowed users to control parameters for recommendations, one could argue that they would enhance consumer autonomy.

At the same time, philosophers[21] and lawyers[22] studying the impacts of AI on society and markets share concerns that, currently, firms using the technology negatively impact consumer autonomy. These concerns mainly relate to privacy issues, such as untransparent or misleading personal data collection and processing. They also reflect on the extent to which algorithms influence consumers' preferences and choices (eg through untransparent advertising and recommendations parameters, users lacking control over these parameters or by making it difficult to withdraw from services). Thus, the issue is not to regulate the technology abstractly but specific commercial practices.

Addressing these issues today is necessary to mitigate possible negative consequences in the near and long term.[23] While these concerns might not qualify as "existential" in the sense of extinguishing humankind, they could significantly alter human nature in terms of free will, personhood, intimacy and interpersonal relationships.[24] Regulators should thus prioritise the protection of consumer autonomy for current and future generations.

[21] M Coeckelbergh, AI Ethics (Cambridge, MA, MIT Press 2020); E Sadin, *L'intelligence artificielle ou l'enjeu du siècle : anatomie d'un antihumanisme radical* (Paris, L'échappée, 2018). On the impacts of digital technologies on personal autonomy, see also Roessler, supra, note 6.

[22] P Hacker, "Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, And Privacy Law" (2021) European Law Journal, doi: 10.1111/eulj.12389; N Helberger, O Lynskey, H-W Micklitz et al, "EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets", report for BEUC, 2021, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf> (last accessed 4 January 2023); Jabłonowska et al, supra, note 8; Mik, supra, note 5.

[23] Many AI experts identify the loss of human agency and control over one's life as some of the main concerns around the development of AI by 2030 (Pew Research Center, *Artificial Intelligence and the Future of Humans* (December 2018) <https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/> (last accessed 4 January 2023)).

[24] Zuboff calls it the "seventh extinction", affecting "what has been held most precious in human nature: the will to will, the sanctity of the individual, the ties of intimacy, the sociality that binds us together in promises, and the trust they breed" (Zuboff, supra, note 6, 516).

Consumers appearing indifferent to protecting their privacy or autonomy is no reason for regulators not to intervene – to the contrary. Indeed, consumers usually face the "privacy paradox": although they constantly *state* that they value privacy, they often do not act to protect it and freely provide their data.[25] Worse: consumers appear to suffer from a cognitive bias known as the "non-belief in the law of large numbers", whereby, due to information overload about the implications of their decisions regarding privacy, they actually *undervalue* it.[26] This apparent lack of concern usually reflects a lack of understanding about the consequences of their technology uses.[27] At the same time, scholars repeatedly demonstrate the case for protecting both privacy[28] and autonomy,[29] adding to the arguments for more regulatory intervention, not less.

The following subsections discuss three commercial practices relying partially or entirely on AI that particularly affect consumer autonomy and are linked together. The starting point of our analysis relates to design choices in user interfaces because they are doorways to more privacy- and autonomy-intrusive practices (Section III.1). This is the case for digital targeted advertising, which AI systems heavily automate (Section III.2), as well as for personalised recommendations (Section III.3).

1. Design choices in user interfaces

Designing user interfaces for technology is not neutral and impacts user engagement. Although design choices are not explicitly related to AI, they are relevant to consider when analysing the effects of AI on consumer autonomy. Indeed, some interfaces are intentionally designed to deceive or manipulate consumers when making decisions such as privacy choices (eg with deceiving cookie banners). Such design choices are more commonly known as "dark patterns".[30] The focus here will be on dark patterns affecting privacy choices. Indeed, in consumer transactions, their use upstream allows firms to obtain more personal data to feed their AI systems, enabling potentially more effective targeted advertising and personalised recommendations downstream (see the following sections).

The use of dark patterns is widespread, including on popular websites. In 2019, researchers developed automated techniques that identified dark patterns on about 11,000 shopping websites worldwide.[31] The study defined dark patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions" – thus, not limited to privacy choices. The authors found that around 11% of these websites contained dark patterns and that they were more likely to appear on popular websites.

Dark patterns affecting privacy choices are illegal, among other things, because they do not comply with the General Data Protection Regulation (GDPR)'s requirements for valid

[25] PA Norberg, DR Horne and DA Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors" (2007) 41(1) Journal of Consumer Affairs 100; A Acquisti, CR Taylor and L Wagman, "The Economics of Privacy" (2016) 54(2) Journal of Economic Literature 476.

[26] IN Cofone and AZ Robertson, "Consumer Privacy in a Behavioral World" (2018) 69(6) Hastings Law Journal 1475.

[27] Q André, Z Carmon, K Wertenbroch et al, "Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data" (2018) 5 Customer Needs and Solutions 28.

[28] N Richards, *Why Privacy Matters* (Oxford, Oxford University Press 2022); Véliz, supra, note 20.

[29] G Wagner and H Eidenmüller, "Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions" (2019) 86(2) University of Chicago Law Review 581.

[30] A Mathur, G Acar, MJ Friedman et al, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" (2019) 3(CSCW) Proceedings of the ACM on Human–Computer Interaction 1.

[31] ibid.

consent, which must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes".[32] Returning to our short conceptualisation of autonomy (see above), the GDPR's requirements for consent imply that consumers – as data subjects – should have a real *choice* about accepting being tracked online. Here, transparency and consent come together because data subjects' consent is only valid if firms duly and intelligibly inform them of their data collection and the purposes of their data processing, enabling them to make that choice. In other words, bypassing transparency requirements directly affects consumer autonomy – in terms of choice, privacy and independence – and makes consent invalid under the GDPR. In 2020, an empirical study showed that so-called "cookie banners" appearing on websites and seeking consumer consent to place cookies on their devices were mainly not compliant with the GDPR: just 11.8% of websites using the five top consent management platforms met minimal GDPR requirements for valid consent.[33]

The French data protection authority referred to this empirical study in its decision to fine Facebook €60 million for the use of dark patterns, namely not enabling users to reject cookies as easily as accepting them.[34] Discouraging users to decline cookies while encouraging them to accept being tracked on the first page undermined their freedom of consent, as many users would not accept cookies if offered a genuine choice. The Commission Nationale de l'Informatique et des Libertés (CNIL) also fined Google €150 million for similar practices.[35] Applying the French law transposing the ePrivacy Directive in light of the heightened consent requirements under Article 4(11) and Recital 42 GDPR, the authority held that the method employed by Google and YouTube for users to manifest their choice over the placing of cookies was illegally biased in favour of consent.[36] Again, the authority referred to several studies showing that organisations implementing a "refuse all" button on the first-level consent interface had seen a decrease in the consent rate to accept cookies.[37] The CNIL more recently fined Microsoft €60 million for similar practices within its Bing search engine, relying on the same studies.[38]

To conclude, the design of digital technologies has important implications for long-term thinking, especially for its impact on consumerism. Philosopher Roman Krznaric argues that the design of digital technologies plays a significant role in consumer autonomy and that short-term design elements – such as the "Buy Now" button – contribute to a culture of instant gratification that can undermine the ability to make autonomous decisions in the long term.[39] Krznaric asserts that technology companies often prioritise immersing users in the digital present, distracting them from pursuing long-term goals.[40] In a way, the French data protection authority recognised just that by finding that Google was discouraging users from rejecting cookies, taking advantage of the fact that Internet browsing is "fast and fluid".[41] The challenge for policymakers is thus to

[32] Art 4(11) GDPR. See also Art 29 Working Party Guidelines on Consent under Regulation 2016/679; Frobrukerrådet, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (last accessed 4 January 2023).

[33] M Nouwens, I Liccardi, M Veale et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence" (2020) Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery 1.

[34] Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2021-024 du 31 décembre 2021.

[35] Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2021-023 du 31 décembre 2021.

[36] ibid, paras 129 and 135.

[37] ibid, para 134.

[38] Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2022-023 du 19 décembre 2022.

[39] R Krznaric, *The Good Ancestor: How to Think Long Term in a Short-Term World* (London, W.H. Allen 2020) p 51.

[40] ibid, 58.

[41] Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2021-023 du 31 décembre 2021, para 135.

foster long-term thinking in regulation and the industry to preserve consumer autonomy, as will be discussed in Section IV.

2. Behavioural advertising

Firms design dark patterns to obtain personal consumer data, usually for advertising purposes. For example, targeting cookies towards consumers' devices allows digital advertisers to track Internet browsing across websites. By crossing this information with personal and behavioural data from social media and data purchased from brokers, digital advertisers use AI systems to analyse consumer preferences. Advertisers can target them with personalised ads by relying on complex networks of actors[42] and having first-hand knowledge of consumer behaviours. For consumers, the benefits of personalised advertisements include lower transaction costs, as the recommended products and services supposedly better match their preferences. However, behavioural advertising raises issues regarding consumer autonomy, especially in terms of privacy, independence and reciprocity, referring to the requirements proposed in Section II.

First, in terms of privacy, digital targeted advertising is highly problematic within the European data protection framework. Being opaque about data processing in privacy policies itself constitutes a GDPR infringement. Veale and Zuiderveen Borgesius argue that real-time bidding (RTB) for ads – behavioural advertising is based on such auctions – is mainly incompatible with EU data protection rules because of the GDPR's transparency and consent requirements.[43] The Belgian data protection authority cited the authors' article in a 2022 decision sanctioning IAB Europe for several GDPR infringements.[44] The case concerned IAB Europe's Transparency and Consent Framework, a widespread mechanism facilitating the management of users' preferences for personalised digital advertising. The authority found that IAB Europe lacked a valid legal basis for processing personal information and was not transparent about the scope of the processing, preventing users from controlling their data. Overall, this decision calls into question the legality of the entire RTB ecosystem considering the GDPR.[45] The Norwegian Consumer Council and other consumer protection groups notably called for a ban on "surveillance-based advertising", arguing that pervasive commercial surveillance online to show personalised ads to consumers cannot justify constant violations of fundamental rights.[46] Again, behavioural advertising in its current form thus appears to undermine core features of consumer autonomy: a lack of privacy or control over their personal data impedes consumers from having more independence in markets and entails risks for society at large (think about targeted political advertising and possible manipulation of the political process).

Second, in terms of independence, issues of transparency and consent with dark patterns upstream also impact consumer autonomy downstream when personal data – for example, data collected with cookies – are used to refine ad targeting. In addition, as more products connect to the Internet, the ability of advertisers to target consumers based on their offline behaviour increases, raising further privacy concerns affecting consumer autonomy, especially in terms of transparency.

[42] M Veale and F Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law" (2022) 23 German Law Journal 226.

[43] ibid.

[44] Belgian Data Protection Authority, Litigation Chamber, Decision on the Merits 21/2022, 2 February 2022.

[45] M Veale, M Nouwens and C Santos, "Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?" (2022) Technology and Regulation 12.

[46] Frobrukerrådet, *Time to Ban Surveillance-Based Advertising: The Case against Commercial Surveillance Online*, (June 2021) <https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf> (last accessed 4 January 2023).

For instance, interactions with voice assistants through connected speakers are highly problematic. An audit of Amazon Echo shows that Amazon and third parties using the smart speaker platform track these interactions, allowing at least Amazon to infer user interests.[47] The study found that Amazon and third parties use this information for personalised, targeted advertising and that advertising parties share these user data significantly. Most importantly, neither Amazon nor third parties are transparent enough about these practices in their privacy policies, with 70% of third parties not even mentioning Amazon or its voice assistant.[48] The study also found that third parties sync their cookies with Amazon and other third parties, demonstrating the importance of dark patterns as a gateway to more autonomy capture, as defined in Section II.[49]

Third, in terms of reciprocity, Internet companies dominating digital advertising markets, thanks to their access to scores of behavioural data, have demonstrated their ability to influence consumer behaviour. For instance, Facebook notably showed in a study that it could manipulate its users' emotions without their awareness[50] – a troubling ability for a company building virtual reality devices and platforms, thanks to which it collects more emotional data for its advertising business.[51] Another study in Vienna suggests that Google Maps influences users' choices of the best transportation type, nudging them into driving their cars.[52] Thus, the personal data not transparently obtained upstream tangibly impact downstream consumer autonomy. However, the reciprocity requirement for consumer autonomy would require more control and complementarity in the relationship between professionals and consumers, which would limit undue commercial influence.

In terms of long-term thinking, influencer marketing poses specific risks for children. What is at stake is the construction of the personality of individuals comprising the next generation of adults. Because they are still developing their personalities, children are more negatively affected than adults by commercial influence.[53]

Empirical research shows that children are particularly vulnerable to online tracking for advertising purposes: mobile apps for children are among the worst in terms of third-party tracking.[54] This tracking allows online platforms to build better profiles of these young users and target them more effectively for marketing purposes. A study requested by the European Parliament shows that children are particularly vulnerable to influencer marketing.[55] Children strongly identifying with influencers tend to imitate their behaviours.[56] The consequences for autonomy are significant: influencer marketing affects brand attachment and future purchases, potentially develops materialistic behaviours, confronts children with inappropriate content and reinforces role perceptions and

[47] U Iqbal, PN Bahrami, R Trimananda et al, "Your Echos Are Heard: Tracking, Profiling, And Ad Targeting in the Amazon Smart Speaker Ecosystem" (2022) <http://arxiv.org/abs/2204.10920> (last accessed 4 January 2023).

[48] ibid.

[49] ibid.

[50] A Kramer, JE Guillory and JT Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks" (2014) 111(24) Proceedings of the National Academy of Sciences of the United States of America 8788.

[51] B Heller and A Bar-Zeev, "The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad" 1(1) Journal of Online Trust and Safety 1.

[52] B Wagner, T Winkler and S Human, "Bias in Geographic Information Systems: The Case of Google Maps" (2021) *Proceedings of the 54th Hawaii International Conference on System Sciences* <https://epub.wu.ac.at/id/eprint/7801> (last accessed 4 January 2023).

[53] For example, children are particularly vulnerable to influencer marketing, which also relies on AI systems (see F Michaelsen, L Collini, C Jacob et al, *The Impact of Influencers on Advertising and Consumer Protection in the Single Market Study* (requested by the IMCO Committee of the European Parliament, February 2022, PE 703.350)).

[54] R Binns, U Lyngs, M Van Kleek et al, "Third Party Tracking in the Mobile Ecosystem" (2018) *Proceedings of the 10th ACM Conference on Web Science* 23 <https://doi.org/10.1145/3201064.3201089> (last accessed 4 January 2023).

[55] Michaelsen et al, supra, note 53.

[56] ibid, 44.

expectations regarding physical appearance. All of these factors ultimately impact the development of children's traits and attitudes, with possible replications in their adult lives. While international law establishes the right to develop one's personality,[57] arguably no other generation has been exposed to this level of targeted and influential marketing. Hence, policymakers and the industry need to give more consideration to the potential harm to the following generations.

Overall, advertisers' extensive collection and processing of behavioural and emotional data to better target users and personalise their services imply significant risks to consumer autonomy, especially in terms of privacy, independence and reciprocity. However, more reciprocity and control by consumers first implies more privacy and independence. The pervasiveness and complexity of digital advertising networks also highlight critical power imbalances and information asymmetries between traders and consumers that are not comparable with pre-AI marketing practices.[58]

3. Personalisation and recommender systems

Consumers increasingly use recommender systems to access personalised content. A 2019 study showed that 41% of music streamed on platforms is recommended by algorithms.[59] Around 70% of videos watched on YouTube and 80% on Netflix are recommended by algorithms.[60] Shopping websites like Amazon extensively use product recommendations too. The current social media trend is to show users more AI-recommended content instead of friends' content. The benefits of personalised recommendations for consumers include displaying potentially relevant content or products, thus enabling them to make sense of vast amounts of information and reducing transaction costs. Nevertheless, recommender systems also present risks for consumer autonomy, especially in terms of privacy, independence and reciprocity, with both individual and collective effects.

First, these recommendations entail privacy risks. More precise recommendations require more personal data – including behavioural data and past consumption habits. As explained above, privacy risks arise when personal data are collected and processed illegally upstream. Like targeted advertising, this untransparent data collection can negatively affect consumer autonomy downstream, as recommendations shown to users are based on illegally obtained personal data.

Second, the requirement for independence, implying more transparency, is undermined because data protection regulation – which mainly establishes individual rights – does not adequately cover the societal risks provoked by personalised services. Societal risks can inter alia relate to political polarisation due to "echo chambers",[61] the perpetuation of unsustainable consumption habits[62] and the erosion of privacy. The issue is that online targeting makes individual situations mainly opaque to other consumers,

[57] Art 29(1)(a) of the UN Convention on the Rights of the Child. See also UN Committee on the Rights of the Child, General comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, 2 March 2021, CRC/C/GC/25, which refers to the importance of preserving children's autonomy in the digital environment.

[58] On this point, see Mik, supra, note 5.

[59] JS Beuscart, S Coavoux and S Maillard, "Les algorithmes de recommandation musicale et l'autonomie de l'auditeur: analyse des écoutes d'un panel d'utilisateurs de streaming" (2019) 213 Réseaux : communication, technologie, société 35.

[60] O Aribaud, *Al(t)gorithmes (1): Des recommandations toujours plus gourmandes en données personnelles ?* (LINC, 17 December 2022) <https://linc.cnil.fr/fr/altgorithmes-1-des-recommandations-toujours-plus-gourmandes-en-donnees-personnelles> (last accessed 4 January 2023).

[61] M Haroon, A Chhabra, X Liu et al, "YouTube, The Great Radicalizer? Auditing and Mitigating Ideological Biases in YouTube Recommendations" (2022) <https://arxiv.org/abs/2203.10666> (last accessed 4 January 2023).

[62] Bjørlo et al, supra, note 2, 9.

civil society organisations, regulators or researchers.[63] Thus, establishing more transparency requirements and individual rights (the right of access, the right to data portability and the right to be forgotten, to name a few) does not help us to deal with more collective problems. Some have criticised the current personal data regulation framework, which mainly focuses on the individual,[64] whereas personalisation also has significant consequences for societal life.[65]

Third, in terms of reciprocity, consumers lack control over these personalised recommendations and over how to modify or influence them. A 2022 report showed how users on YouTube – the second most visited website worldwide – feel that they do not have control over its recommendations, despite the platform having implemented feedback tools.[66] Empirical data from the largest experimental audit of the platform confirm this feeling: user controls are mostly ineffective at preventing undesirable recommendations. Consumers primarily use passive ways of influencing recommender systems through feedback tools (eg by liking, flagging if the content is not relevant to them or following accounts) but currently lack more active ways of influencing them.[67] Such recommendations lack true bi-directionality, thus undermining complementarity as one of the characteristics of consumer autonomy discussed above.[68] More active ways to influence recommender systems could include more control over the specific parameters for those recommendations.

In terms of long-term thinking, recommender systems also impact culture as such, which ultimately amounts to achievements of human intellect transmitted from generation to generation. As human culture is increasingly transmitted in the digital world, including through recommender systems, what place do algorithms take in this transmission? Do recommender systems have any bias in cultural transmission? Cultural evolution researchers are increasingly examining these questions,[69] as they might have long-term impacts on cultural transmission.

IV. Mapping and assessment of EU regulatory instruments

After discussing the risks posed by specific commercial practices, the question is whether and to what extent current EU regulation considers the long-term consequences of using AI systems on consumer autonomy. This section maps EU regulatory instruments addressing consumer autonomy, considering their long-term implications for the three commercial practices discussed above. Figure 2 shows the principal fundamental rights involved and the new regulatory landscape applied to the three practices highlighted above: (1) design choices in user interfaces; (2) behavioural advertising; and (3) personalisation and recommender systems.

[63] Authors have pointed out that online targeting entails risks of epistemic fragmentation, defined as the "lack of shared context in relation to a given practice of content personalisation" (S Milano, B Mittelstadt, S Wachter and C Russell, "Epistemic Fragmentation Poses a Threat to the Governance of Online Targeting" (2021) 3 Nature Machine Intelligence 466). In addition, a report on YouTube's recommender system explains that personalisation was difficult to study without accessing real user data. It calls on policymakers to protect public interest research (B Ricks and J McCrosky, "Does This Button Work? Investigating YouTube's ineffective user controls" (*Mozilla Foundation*, September 2022) 37–38 <https://foundation.mozilla.org/en/research/library/user-controls/report/> (last accessed 4 January 2023).

[64] M Finck, "The Limits of the GDPR in the Personalisation Context" (2021) *Max Planck Institute for Innovation & Competition Research Paper No. 21-11*.

[65] Sadin, supra, note 21; Helberger et al, supra, note 22, 27.

[66] Ricks and McCrosky, supra, note 63.

[67] Bjørlo et al, supra, note 2, 9.

[68] ibid, 8.

[69] L Brinkmann, D Gezerli, KV Kleist et al, "Hybrid Social Learning in Human–Algorithm Cultural Transmission" (2022) 380(2227) Philosophical Transactions of the Royal Society A 20200426.

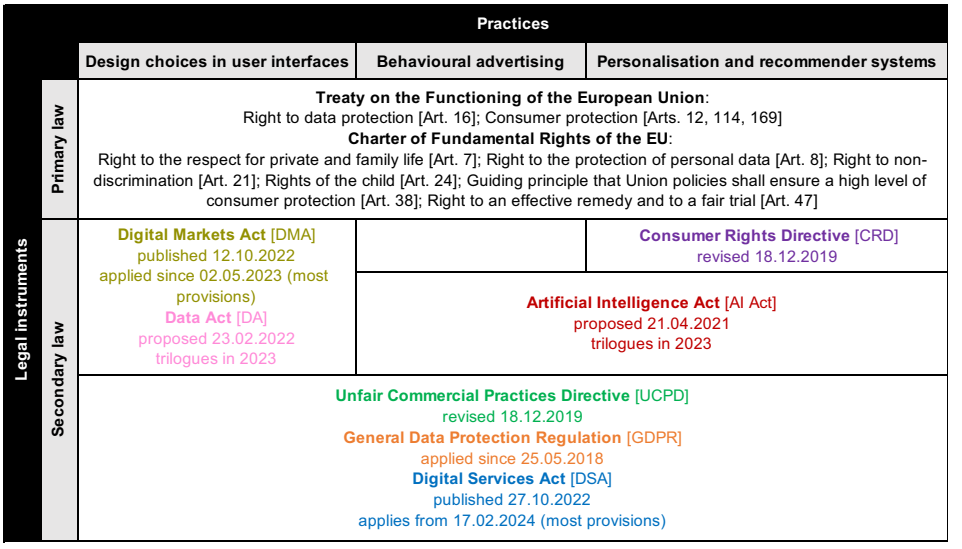

Figure 2. Overview of the European Union (EU) regulatory landscape.

1. Autonomy

In the EU, protecting consumer autonomy has never been the main objective but rather a means to instrumentalise private law for market integration.[70] The main techniques of EU private law to that end have been information duties,[71] a light regulatory intervention and a small price to pay for traders to access one of the largest consumer markets. Today, digital economy regulation continues to require important information disclosures to achieve more transparency, but the EU legislator also establishes more prohibitions and specific obligations for traders to protect consumers from the risks highlighted above. Figure 3 offers an overview of EU regulations aiming at protecting consumers against these risks.

As Figure 3 shows, relevant instruments proceed from consumer, data protection and competition law. Many of these instruments already apply. That is the case of the GDPR,[72] the Unfair Commercial Practices Directive (UCPD)[73] and the Consumer Rights Directive (CRD)[74] – the latter two were slightly revised in 2019. However, instruments recently adopted or in the legislative pipeline establish new rules affecting all three commercial

[70] HW Micklitz and D Patterson, *From the Nation State to the Market: The Evolution of EU Private Law*, EUI LAW, 2012/15, 12 <http://hdl.handle.net/1814/22415> (last accessed 4 January 2023).

[71] See information requirements in the Unfair Commercial Practices Directive, the Consumers Rights Directive and the General Data Protection Regulation.

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp 1–88.

[73] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, OJ L 149, 11.6.2005, pp 22–39.

[74] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, pp 64–88.

<table>
<tr><th colspan="2" rowspan="2">Focus: Autonomy</th><th colspan="3">Practices</th></tr>
<tr><th>Design choices in user interfaces</th><th>Behavioural advertising</th><th>Personalisation and recommender systems</th></tr>
<tr><td colspan="2" rowspan="2">Prohibition for online platforms to design online interfaces to deceive, manipulate or materially distort or impair free and informed decisions [Art. 25 + Recital 67 DSA] but not for practices covered by UCPD or GDPR

Prohibition for gatekeepers to engage in behaviour undermining prohibitions of DMA, incl. by subverting end users' autonomy, decision-making, or free choice via the design of user interface [Art. 13(6) DMA]

Prohibition for third parties to whom data is made available to coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, incl. with user interface [Art. 6(2)(a) DA]</td><td>Misleading practice: search results without disclosing paid ad [Annex I, 11a UCPD]

Transparency over advertising in general: marking as ad (e.g., influencers) and main parameters for targeting and how to change them [Art. 26(1) DSA]

Prohibition of using special categories of sensitive data for profiling for targeted advertising [Art. 26(3) DSA]

Prohibition of children profiling for targeted advertising [Art. 28(2) DSA]

Public ad repository (info on content, origin and who paid, period displayed, parameters for presenting to specific group, recipients reached) [Art. 39 DSA]</td><td>Online platforms using recommender systems need to indicate the main parameters (criteria and reasons for relative importance) in terms and conditions + options to modify or influence those parameters, incl. through a functionality in settings [Art. 27 DSA]

Option not to be profiled for each recommender system on very large online platforms [Art. 38 DSA]

Information requirement: price was personalised on the basis of automated decision-making [Art. 6(1)(ea) CRD]</td></tr>
<tr><td colspan="2">Right not to be subject to decision solely based on automated processing, incl. profiling, producing legal effects or significantly affecting data subject [Art. 22 GDPR] + controller to provide information about existence of automated decision-making, logic involved, and significance and consequences of processing for data subject [Art. 13 + 14 GDPR] + right of access [Art. 15 GDPR] + right to object [Art. 21 GDPR]

Prohibition of subliminal techniques and manipulative AI systems materially distorting behaviour, causing or likely to cause physical or psychological harm [Art. 5(1) AI Act]

Transparency requirements for AI systems: (i) interaction with AI system; (ii) emotion recognition or biometric categorisation systems; (iii) deep fakes [Art. 52 AI Act]</td></tr>
<tr><td colspan="3">Prohibition of misleading + aggressive commercial practices [Art. 8 UCPD]: undue influence (exploiting a position of power) significantly impairing or is likely to significantly impair the average consumer's freedom of choice or conduct and thereby causes him/her or is likely to cause him/her to take a transactional decision that he/she would not have taken otherwise</td></tr>
</table>

Figure 3. Overview of European Union (EU) regulations related to consumer autonomy in the artificial intelligence (AI) context. AI Act = Artificial Intelligence Act; CRD = Consumer Rights Directive; DA = Data Act; DMA = Digital Markets Act; DSA = Digital Services Act; GDPR = General Data Protection Regulation; UCPD = Unfair Commercial Practices Directive.

practices. Most provisions of the Digital Markets Act (DMA)[75] have applied since May 2023. Similarly, most provisions of the Digital Services Act (DSA)[76] will apply from February 2024. The Artificial Intelligence Act (AI Act) entered trilogue negotiations in 2023, so there is still time before its application.

One regulatory instrument does apply horizontally to all three practices at hand: the UCPD. Although the UCPD prohibits misleading and aggressive commercial practices, the main issue highlighted in the literature is the standard against which to assess a particular practice: that of the average consumer and their understanding under the case law of the Court of Justice of the European Union (CJEU). Indeed, authors have called into question the use of the average consumer standard, arguing that it is not suitable to address the

[75] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, pp 1–66.

[76] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, pp 1–102.

extent of the power imbalances and asymmetry of information in the digital realm.[77] This is because the definition of the vulnerable consumer – to whom the Directive attaches more robust protection compared to the average consumer – only used to take into account specific categories of consumers, solely based on their internal characteristics, not considering exposure to external factors.[78] However, the Commission adopted new guidelines on the interpretation of the UCPD in late 2021, which regard the concept of vulnerability in data-driven practices and dark patterns as "dynamic and situational". Although this guidance is welcome, as it seems better adapted to the digital realm, its concrete application in cases is still to be analysed by the CJEU.

a. Design choices in user interfaces

If most of the literature and enforcement action focuses on applying data protection rules to tackle dark patterns, scholars have also shown how consumer protection instruments – especially the UCPD – can help counter them.[79] In 2021, the Commission adopted new guidelines on the application of the UCPD that consider "data-driven practices and dark patterns",[80] which are expected to better assess the vulnerability of consumers depending on the situation at hand.

New instruments will soon apply. First, the DSA prohibits online platforms from designing interfaces to deceive, manipulate or materially distort or impair free and informed decisions. While this prohibition seems helpful at first, it has two significant limitations. First, the prohibition only concerns online platforms, not intermediaries, contrary to what was initially intended, considerably limiting the scope of this rule, especially given the widespread use of dark patterns online, and not only by prominent actors. Second, the prohibition does not apply to practices covered by the UCPD or the GDPR.[81] Although the provision requires further interpretation, this second limitation seems to annihilate the prohibition, as most dark patterns are illegal under either instrument.[82]

Second, the DMA and the Data Act[83] include similar prohibitions against manipulative designs. Under the DMA, gatekeepers of digital platforms cannot use dark patterns to undermine the Regulation's prohibitions. Under the proposal for a Data Act – designed to foster data sharing in the advent of the Internet of Things – third parties to whom data are made available cannot use manipulative designs either.

Overall, although the current data and consumer protection law regime already offers ways of tackling the use of dark patterns, these new prohibitions might be helpful to clarify the obligations of each actor under these new regulatory regimes. They also introduce new pathways for private and public enforcement – with the Commission having a central role in enforcing the DSA, for instance – multiplying the possibilities of tackling dark patterns. These new regimes are welcome to preserve consumer autonomy regarding the choice requirement proposed in Section II, but their concrete application still needs to be studied.

[77] Helberger et al, supra, note 22, 8 et sqq. See also F Esposito and M Grochowski, "The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration" (2022) 18(1) European Review of Contract Law 1.

[78] Helberger et al, supra, note 22, 8 et sqq.

[79] MR Leiser and MM Caruana, "Dark Patterns: Light to be Found in Europe's Consumer Protection Regime" (2021) 10(6) Journal of European Consumer and Market Law 237.

[80] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, C/2021/9320, OJ C 526, 29.12.2021, pp 1–129 (hereafter, "Commission UCPD Guidance").

[81] Art 25 of the Digital Services Act.

[82] Commission UCPD Guidance, note 80, section 4.2.7.

[83] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23.2.2022.

b. Behavioural advertising

The existing regulatory framework already contains rules limiting behavioural advertising.[84] Data protection authorities progressively enforce the GDPR for issues related to digital advertising,[85] which might prompt adtech actors to review their practices in terms of consent and transparency, hopefully providing more privacy and independence to consumers. As developed in Section II, privacy protection upstream is indeed a requirement for more consumer independence and reciprocity downstream. Notably, the European Data Protection Board instructed the Irish data protection authority to fine Meta €390 million for using an invalid legal basis for processing its users' data for personalised advertising purposes.[86] Facebook and Instagram have relied on the performance of a contract (their terms of service) instead of relying on consent to process such data. The European Data Protection Board found that social media could not rely on the "contract legal basis" for behavioural advertising purposes and that users should be able to opt out of personalisation.

New instruments (will) impose additional obligations. The DSA now establishes more stringent and explicit rules applicable to targeted advertising, partly incorporating concerns from academia and consumer organisations. For instance, the DSA limits targeted advertising's most evident and severe issues, such as targeting based on sensitive personal data or targeting children using any kind of personal data. The AI Act proposal prohibits using "subliminal techniques" and "manipulative AI systems" that materially distort behaviour or (likely) cause physical or psychological harm. However, it is as yet unclear whether this wording would encompass personalised advertising.[87]

Although the UCPD already applies to influencer marketing,[88] the EU legislator incorporated new obligations in this field. Indeed, scholars have pointed out that one of the Act's blind spots is related to new models of advertising based on content monetisation and "human ads".[89] After the European Parliament incorporated significant amendments, the DSA now imposes on providers of online platforms to ensure that influencers mark their posts as "ads" when promoting products or services and provide information about them. The added value of the DSA compared to the UCPD relies on the former imposing this obligation on online platforms themselves (while the UCPD is addressed to influencers directly), thus increasing possibilities of compliance mechanisms and enforcement.

Interestingly, the DSA requires very large online platforms to present a public ad repository containing information on the ad's content and origin (including who paid for it), the period during which it was displayed, the parameters for presenting it to specific groups and the total number of recipients reached and where (breakdown by Member State). If this provision might have limited use for individual consumers, it will no doubt be of immense use for regulators, consumer protection organisations and researchers. It also has the potential to mitigate the effects of epistemic fragmentation produced by behavioural advertising and personalisation, as described above.

[84] Commission UCPD Guidance, supra, note 80, sections 4.2.1 and 4.2.5; Veale and Zuiderveen Borgesius, supra, note 42.

[85] Veale et al, supra, note 45.

[86] Irish Data Protection Commission, *Data Protection Commission announces conclusion of two inquiries into Meta Ireland* (4 January 2023) <https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland> (last accessed 4 January 2023); V Manancourt, *€390M fine strikes blow to Meta's ad-fueled business model* (*POLITICO*, 4 January 2023), <https://www.politico.eu/article/meta-fina-ad-business-model/> (last accessed 4 January 2023).

[87] D Bomhard and M Merkle, "Regulation of Artificial Intelligence: The EU Commission's Proposal of an AI Act" (2021) 10(6) Journal of European Consumer and Market Law 259.

[88] Commission UCPD Guidance, supra, note 80, section 4.2.6.

[89] C Goanta, "Human Ads Beyond Targeted Advertising: Content Monetization as the Blind Spot of the Digital Services Act" (*Verfassungsblog*, 5 September 2021) <https://verfassungsblog.de/power-dsa-dma-11/> (last accessed 4 January 2022).

c. Personalisation and recommender systems

Much had been expected from the GDPR to better protect consumers willing to escape personalisation, but the initial years of its enforcement have demonstrated its limits.[90] Paradoxically, although the GDPR is based on the principle of informational self-determination, thus presupposing consumer autonomy, individual rights might not always be appropriate to regulate such complex situations of personalisation.[91] Privacy rights in the GDPR only consider the data provided, not the data generated or inferred based on that data.[92] In other words, consent is not only flawed for data obtained through dark patterns, but it is, bluntly, non-existent for inferred data. Arguably, inferred data provide even greater insights than explicitly stated data (which can be purposely inaccurate), as big data and AI allow for probabilistic determinations. This realisation prompted ethicists to call for a new data protection right: a right to reasonable inferences,[93] requiring data controllers to justify their inferences ex ante and the ability for individuals to challenge them ex post.

Thus, compliance with the new rules introduced by the DSA will be closely scrutinised, all the more so that they impose obligations on platforms themselves and allow individuals to understand better how recommendations are personalised for them and how to change them. The DSA indeed obliges online platforms to indicate the main parameters used for recommendations, including the criteria used and the reasons for their relative importance. The only problem is that online platforms must add this transparency requirement in their terms and conditions, which consumers largely ignore.[94] However, this limitation is mitigated by the fact that online platforms will have to offer options to modify or influence the parameters on which they base their recommender systems through additional functionality in their settings. Depending on the implementation of such functionalities, they might contribute to increasing consumer autonomy, as they would be able to influence actively the recommended content depending on their evolving preferences. Hopefully, these features could better "accommodate for [consumers'] aspirational preferences".[95] Additionally, very large online platforms must include an option not to be profiled for each recommender system. This last rule is welcome to increase consumer autonomy, as Article 22 of the GDPR, which establishes the right not to be subject to decisions solely based on the automated processing of personal data, including profiling, is more limited in scope *ratione materiae* (not *ratione personae*).

2. *Long-term thinking*

Current policymaking related to consumer autonomy still appears to lack long-term thinking. Although the European Commission recognises that current data policies will affect the following decades, the European Strategy for Data adopted in 2020 outlines policies for the following five years only.[96] Although civil society organisations had conveyed to the Commission the need to establish future-proof digital principles and prevent "negative effects of long-term exposure to digital technologies",[97] its proposal for

[90] Finck, supra, note 64.

[91] ibid.

[92] Zuboff, supra, note 6, 480–88.

[93] S Wachter and B Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" (2019) 2 Columbia Business Law Review 1.

[94] Bakos et al, supra, note 17.

[95] Bjørlo et al, supra, note 2, 9.

[96] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM(2020) 66 final, 19.02.2020.

[97] Commission Working Staff Document, Report on the stakeholder consultation and engagement activities, accompanying the document "Establishing a European Declaration on Digital rights and principles for the Digital Decade", SWD(2022) 14 final, 26.1.2022, pp 24–25.

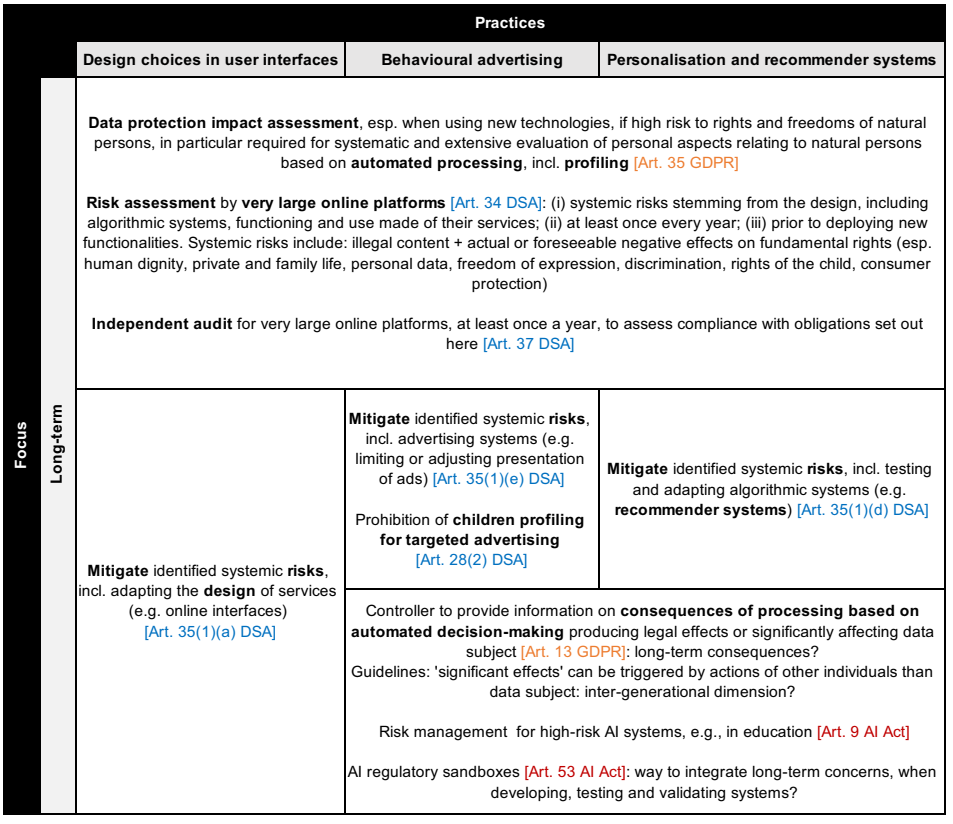

Figure 4. Overview of European Union (EU) regulations related to long-term thinking for consumer autonomy in artificial intelligence (AI)-intensive markets. AI Act = Artificial Intelligence Act; DSA = Digital Services Act; GDPR = General Data Protection Regulation.

a Declaration on European Digital Rights and Principles failed to incorporate such concerns.[98] While the new EU regulatory instruments identified here address critical issues related to consumer autonomy, their ability to address these long-term implications appears more limited. The question is not whether regulations are future-proof from an institutional viewpoint, but whether EU regulations account for consumer autonomy in AI-intensive markets long term, based on the abovementioned risks. As Figure 4 shows, three regulations contain measures that can foster long-term thinking, mainly from the industry: the GDPR, the DSA and the AI Act. The measures highlighted can be classified into two groups: risk assessment obligations and information requirements.

First, most measures relate to obligations to conduct risk assessment. The GDPR currently obliges data controllers to conduct data protection impact assessments, especially before using new technologies involving the processing of large amounts of data, which result in high risks for the rights and freedoms of data subjects. If these risks are too high, the controller should refer its doubts to the supervisory authority. Similarly, the DSA imposes on very large online platforms to conduct risk assessments for their systems, including user interfaces and AI systems such as those used for targeted

[98] European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, 26.1.2022. However, the Declaration's third chapter does include autonomy-preserving principles related to individuals' freedom of choice in interactions with algorithms and AI systems.

advertising and personalised recommendations. In particular, very large online platforms must assess: (1) systemic risks stemming from the design (including algorithmic systems), functioning and use made of their services; (2) at least once every year; and (3) before deploying new functionalities. Under the DSA, systemic risks include illegal content and actual or *foreseeable* adverse effects on fundamental rights (especially human dignity, private and family life, personal data, freedom of expression, discrimination, the rights of the child and consumer protection). The annual independent audit, which very large platforms must undergo under the DSA, does include a review of this risk assessment. Importantly, very large platforms need to mitigate the identified systemic risks, a general obligation that would need further interpretation over its application in practice. Nevertheless, the fact that the regulation imposes on Internet companies to consider *foreseeable* systemic risks shows the will to instil more long-term thinking in the industry. Moreover, the AI Act also imposes risk management obligations for high-risk AI systems but limits them to specific sectors such as education. Finally, one can wonder whether the regulatory sandboxes foreseen in the AI Act might be an appropriate setting to address long-term autonomy concerns, especially when developing, testing and validating AI systems.

The main issue with risk assessments is that they mainly rely on self-assessment. Risk assessments should thus be subject to external review to be meaningful. In that sense, the obligation to conduct an annual audit established by the DSA provides an improvement compared to the risk assessment requirements under the GDPR. The newly launched European Centre for Algorithmic Transparency could also assist the Commission when enforcing the new obligations under the DSA.

Second, information requirements can also be measures through which regulators could impose more long-term thinking from the industry. Indeed, the GDPR could be interpreted this way. According to a transparency requirement in the GDPR, the data controller must provide information on the consequences of processing personal data based on automated decision-making that produces legal effects or significantly affects data subjects. Should this requirement include information on the foreseeable, long-term consequences of automated data processing? To what extent should data controllers conduct this assessment? As stated in the Working Party Guidelines, "significant effects" over automated processing can be triggered by the actions of other data subjects. The Guidelines provide the example of a data subject having their credit card limit reduced due to the automated personal data processing of subjects in the same living area. Could we interpret this provision so that these significant effects also include an intergenerational dimension? For example, could the controller be required to provide information on the foreseeable or possible long-term consequences of its systems? If an AI system engaged in recommending personalised investments inter alia based on personal data, the controller could be required to inform consumers about possible long-term effects of those investments, for the individual and society. The inclusion of the intergenerational dimension in the transparency requirement would encourage the AI platform to consider sustainable and socially responsible investment options. It would also foster a more long-term thinking approach from the industry, aligning with the principles of the GDPR and safeguarding the interests of present and future generations. These questions would require further interpretation, including by the CJEU.

In summary, some measures could instil more long-term thinking from the industry, but their concrete application requires further interpretation. They could also remain a dead letter if not adequately enforced. The advantage of risk assessment obligations over information requirements is that they mitigate harms upstream when products and services are not yet placed on the market.

V. Conclusion: perspectives for integrating consumer autonomy and long-term concerns in AI regulations

Overall, EU regulations addressing autonomy issues in the context of AI use in consumer markets do not sufficiently consider the long-term risks to human nature highlighted in Sections II and III. To ensure these risks are considered, EU policymakers must integrate long-term thinking into consumer and data protection regulations. Adopting such regulations with the long term in mind might become a constitutional requirement if intergenerational solidarity is incorporated into the Treaties, as Commission President von der Leyen suggested in her 2022 State of the Union address.[99] EU regulation can promote long-term thinking differently, depending on whom it targets.

First, regulatory measures can target firms using AI systems. Section IV explained that the GDPR and DSA require Internet companies to conduct data protection and systemic risk assessments. Here, regulation could require Internet companies that train algorithms (eg recommender systems) to consider long-term risks, even for future generations. One could argue that the GDPR suggests just that when it mentions that personal data processing should be designed to serve "mankind" (ie humans collectively, arguably present and future).[100] Recent research suggests that AI trainers adopt more prosocial behaviours when they are aware of the consequences of their actions for future generations.[101] However, this study shows that this is true only when there is a risk of future algorithmic choices harming AI trainers themselves. That limitation alone is a further argument to promote more reflection on the impacts of AI systems on future human conditions as, currently, regard for the long-term consequences of AI applications does not seem to be the focus of their developers.

Second, engineers can be subject to technical measures integrating mandates into their design processes. Studies have illustrated that the GDPR's privacy protocols may be transformed into such demands via socio-technical security modelling language.[102] Addressing privacy and long-term requirements in an interdisciplinary way[103] is even more necessary in this context. Indeed, regulation alone will never be effective if the engineers building AI systems do not have concrete models to implement sometimes abstract rules in a language that they do not master. So-called "requirement engineering" can help software developers build compliant systems by design. Different techniques exist for this objective, one being modelling languages and model-driven engineering; it could also help introduce long-term thinking in the engineering process.

Third, long-term thinking can also be instilled in policymakers themselves. In its Better Regulation Guidelines, the Commission indicates that its impact assessments should consider "possible long-term developments, trends and challenges (using foresight elements and scientific advice, where appropriate)", "take account of the key long-term challenges and corresponding EU policy ambitions" when evaluating a specific problem and "compare the options with regard to their effectiveness, efficiency and coherence, compliance with the proportionality principle and how future-proof they are, given the

[99] European Commission, *2022 State of the Union Address by President von der Leyen* (14 September 2022) <https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493> (last accessed 4 January 2023).

[100] See Recital 4 GDPR.

[101] V Klockmann, A von Schenk and MC Villeval, "Artificial Intelligence, Ethics, and Intergenerational Responsibility" (2022) 203 Journal of Economic Behavior & Organization 284.

[102] C Negri-Ribalta, R Noel, N Herbaut et al, "Socio-Technical Modelling for GDPR Principles: An Extension for the STS-ml" (2022) *30th IEEE International Requirements Engineering Conference* <https://doi.org/10.1109/REW56159.2022.00052> (last accessed 8 May 2023); M Robol, M Salnitri and P Giorgini, "Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework" (2017) *PoEM 2017: The Practice of Enterprise Modeling* 236.

[103] The need to conduct interdisciplinary research on the impacts of AI on consumer protection is further highlighted by European private law experts: see Jabłonowska et al, supra, note 8.

long-term challenges".[104] These requirements for EU policymakers are of paramount importance to preserve consumer autonomy in markets heavily reliant on algorithmic decision-making, especially given the Brussels effect (ie the ability for EU regulation to influence global markets, as the adoption of the GDPR has shown).[105]

However, these guidelines already exist and do not appear to be very effective at incorporating long-term thinking in regulation. Policymakers could use another principle. Here, environmental and health law – which also regulates long-term risks – can help us to draw a parallel. In particular, the precautionary principle has developed in environmental law in the face of uncertainty about future harmful impacts to protect the environment in the long term.[106] According to this principle, regulatory action should be taken even without conclusive scientific evidence as to the potential effects of a particular practice. Just as environmental and health risks can be uncertain, risks of autonomy capture by professionals using AI systems can also be long term. When there is insufficient evidence regarding the harmful effects of an activity on consumer autonomy but strong evidence suggests that the consequences could harm individual and collective autonomy, EU policymakers should apply the precautionary principle.

Although further research is required, mobilising this principle in the field of digital technologies regulation could be appropriate given the high risks to human nature posed by AI systems in consumer markets, as well as the pace of technological development in the AI field, which leaves little time to assess risks before deploying AI systems and regulating them properly. The High-Level Expert Group on Artificial Intelligence recommends adopting a precautionary approach when AI applications involve unacceptable or substantial risks.[107] The European Commission recommends that measures taken based on this principle be proportionate, considering not only immediate risks but also those for future generations.[108] Civil society organisations could also use the principle in strategic litigation to urge public authorities to act accordingly. If applying the precautionary principle could potentially hinder innovation, its increased use in guiding policymakers and the industry would demonstrate a commitment to fundamental rights and the ability to think long term.[109]

Acknowledgements. The author would like to thank Alberto Alemanno, Marco Almada, Mireia Artigot i Golobardes, Rose Campion, Claudia Negri-Ribalta, Luke Newberry, Alessandro Spina and Bas Heerma van Voss for their feedback on previous drafts, including at the Workshop on Long Term Risks and Future Generations held at Maastricht University's campus in Brussels on 23 January 2023.

Competing interests. The author declares none.

[104] European Commission, Commission Staff Working Document, Better Regulation Guidelines, 3.11.2021, SWD(2021) 305 final, pp 31–32.

[105] A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford, Oxford University Press 2020) p 131.

[106] F Ewald, N de Sadeleer and C Gollier, *Le principe de précaution* (Paris, Presses Universitaires de France 2008).

[107] High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendations for Trustworthy AI (European Commission 2019) pp 37–38.

[108] Communication from the Commission on the precautionary principle, COM(2000) 1 final, 2.2.2000, 7, 18.

[109] On this point, see E Lievens "Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights" (2021) 39(2) Nordic Journal of Human Rights 145.

Cite this article: S Fassiaux, "Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2023.58